敏惠醫護管理專科學校

「資訊安全管理系統」
資訊安全政策

機密等級：一般
編　　號：IS-MHCHCM-01-001
版本編號：1.1
制訂日期：112.10.30
使用本文件前，如對版本有疑問，請與修訂者確認最新版次。

資訊安全政策					
文件編號	IS-MHCHCM-01-001	機密等級	一般	版次	1.1

本文件歷次變更紀錄：

版次	修訂日	修訂者	說　　明	核准者
1.0	110.12.30	資訊安全執行小組	初版發行	召集人
1.1	112.10.30	資訊安全執行小組	修訂頁首、頁尾、範圍、定義、資訊安全政策、目標、責任、審查	召集人

本程序書由資訊安全執行小組負責維護。

目錄：

1 目的

1.1 敏惠醫護管理專科學校（以下簡稱本校）為強化資訊安全管理，確保所屬之資訊資產的機密性、完整性及可用性，以提供本校之資訊業務持續運作之資訊環境，並符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之威脅，特定此政策規範。

2 適用範圍

2.1 本校所有單位。

2.2 資訊安全管理涵蓋 4 類控制措施、93 項管理事項，避免因人為疏失、蓄意或天然災害等因素，導致資料不當使用、洩漏、竄改、破壞等情事發生，對本校帶來各種可能之風險及危害。管理事項如下：

2.2.1 組織控制措施：

2.2.1.1 資訊安全政策。
2.2.1.2 資訊安全之角色及責任。
2.2.1.3 職務區隔。
2.2.1.4 管理階層責任。
2.2.1.5 與權責機關之聯繫。
2.2.1.6 與特殊關注群組之聯繫。
2.2.1.7 情資威脅。
2.2.1.8 專案管理之資訊安全。
2.2.1.9 資訊及其他相關資產之清冊。
2.2.1.10 可接受使用資訊及其他相關聯資產。
2.2.1.11 資產之歸還。
2.2.1.12 資產之分類分級。
2.2.1.13 資訊之標示。
2.2.1.14 資訊傳送。
2.2.1.15 存取控制。
2.2.1.16 身分管理。
2.2.1.17 鑑別資料。
2.2.1.18 存取權限。

2.2.1.19 供應者關係中之資訊安全。
2.2.1.20 於供應者協議中闡明資訊安全。
2.2.1.21 管理 ICT 供應鏈中之資訊安全。
2.2.1.22 供應者服務之監視、審查及變更管理。
2.2.1.23 使用雲端服務之資訊安全。
2.2.1.24 資訊安全事故管理規劃及準備。
2.2.1.25 資訊之評鑑及決策。
2.2.1.26 對資訊安全事故之回應。
2.2.1.27 由資訊安全事故中學習。
2.2.1.28 證據之蒐集。
2.2.1.29 中斷期間之資訊安全。
2.2.1.30 營運持續之 ICT 備妥性。
2.2.1.31 法律、法令、法規之契約要求事項。
2.2.1.32 智慧財產權。
2.2.1.33 紀錄之保護。
2.2.1.34 隱私及個人可識別資訊(PII)保護。
2.2.1.35 資訊安全之獨立審查。
2.2.1.36 資訊安全政策、規則及標準的遵循性。
2.2.1.37 書面紀錄之運作程序。

2.2.2 人員控制措施：
2.2.2.1 篩選。
2.2.2.2 聘用條款及條件。
2.2.2.3 資訊安全認知、教育和訓練。
2.2.2.4 獎懲過程。
2.2.2.5 聘用終止或變更後之責任。
2.2.2.6 機密性或保密協議。
2.2.2.7 遠端工作。
2.2.2.8 資訊安全事件通報。

2.2.3 實體控制措施：
2.2.3.1 實體安全周界。
2.2.3.2 實體進入。

2.2.3.3 保全辦公室、房間及設施。
2.2.3.4 實體安全監視。
2.2.3.5 防範實體及環境威脅。
2.2.3.6 於安全區域內工作。
2.2.3.7 桌面淨空及螢幕淨空。
2.2.3.8 設備安置及保護。
2.2.3.9 場所外資產之安全。
2.2.3.10 儲存媒體。
2.2.3.11 支援公用服務事業。
2.2.3.12 佈纜安全。
2.2.3.13 設備維護。
2.2.3.14 設備汰除或重新使用之保全。

2.2.4 技術控制措施：

2.2.4.1 使用者終端設備。
2.2.4.2 特殊存取權限。
2.2.4.3 資訊存取限制。
2.2.4.4 對原始碼之存取。
2.2.4.5 安全識別。
2.2.4.6 容量管理。
2.2.4.7 防惡意軟體。
2.2.4.8 技術脆弱性管理。
2.2.4.9 組態管理。
2.2.4.10 資料刪除。
2.2.4.11 資料遮蔽。
2.2.4.12 資料洩漏預防。
2.2.4.13 資料備份。
2.2.4.14 資訊處理設施之備援。
2.2.4.15 日誌紀錄。
2.2.4.16 監視活動。
2.2.4.17 鐘訊同步。
2.2.4.18 具特殊權限共用程式之使用。

2.2.4.19 對運作中系統之軟體安裝。
2.2.4.20 網路安全。
2.2.4.21 網路服務的安全性。
2.2.4.22 網路區隔。
2.2.4.23 網頁過濾。
2.2.4.24 加密技術之使用。
2.2.4.25 開發生命週期之安全。
2.2.4.26 應用程式安全要求。
2.2.4.27 安全系統架構及工程原則。
2.2.4.28 安全程式設計。
2.2.4.29 開發和驗收中的安全測試。
2.2.4.30 委外開發。
2.2.4.31 開發、測試及運作環境之區隔。
2.2.4.32 變更管理。
2.2.4.33 測試資訊。

2.2.5 在稽核測試期間的資訊系統保護。

本校之內部人員、委外服務廠商與訪客皆應遵守本政策。

3 定義

3.1 資訊資產：係指為維持本校資訊業務正常運作之硬體、軟體、服務、文件及人員。

3.2 營運持續運作之資訊環境：係指為維持本校各項業務正常運作所需之電腦作業環境。

4 願景與目標

4.1 資訊安全政策：

強化資訊安全管理，確保所屬之資訊與資訊資產的機密性、完整性及可用性，以提供本校之資訊業務持續運作之資訊環境，並符合相關法規之要求，使其免於遭受內、外部的蓄意或意外之威脅。

4.2 資訊安全目標：

4.2.1 辦理資訊安全教育訓練，推廣人員資訊安全之意識與強化其對相關責任之認知。

4.2.2 保護本校業務活動資訊，避免未經授權的存取與修改，確保其正確完整。

4.2.3 本校之業務活動執行須符合相關法令或法規之要求。

4.2.4 執行資訊安全風險評估機制，提升資訊安全管理之有效性與即時性。

4.2.5 定期進行資訊安全內部稽核作業，確保相關作業皆能確實落實。

4.2.6 維持資訊系統持續運作確保本校具備可供業務持續運作之資訊環境。

4.3 應針對上述資訊安全目標，擬定年度待辦事項、所需資源、負責人員、預計完成時間以及結果評估方式與評估結果，相關監督與量測程序，應遵循本校「監督與量測管理程序書」辦理。

4.4 資訊安全執行小組應於管理審查會議中，針對資訊安全目標有效性量測結果，向資訊安全委員會召集人進行報告。

5 責任

5.1 本校的管理階層建立及審查此政策。

5.2 資訊安全執行小組透過適當的標準和程序以實施此政策。

5.3 所有人員和委外服務供應商均須依照相關安全管理程序以維護資訊安全政策。

5.4 所有人員有責任報告資訊安全事件和任何已鑑別出之弱點。

5.5 任何危及資訊安全之行為，將視情節輕重追究其民事、刑事及行政責任或依本校之相關規定進行懲處。

6 審查

6.1 本政策應至少每年審查乙次，以反映政府法令、技術及業務等最新發展現況，以確保本校營運持續運作及資訊安全實務作業能力。

7 實施

7.1 任何機關單位因業務需求取得本校機敏性資訊或個人資料時，應負起資料保密責任及妥善運用，並遵守國家相關之法

令及本校之相關資訊安全規定。

7.2 若因機關單位疏失造成資料外洩或資安事件，應負相關法律責任。

7.3 資訊安全政策配合管理審查會議進行審核。

7.4 本政策經「資訊安全委員會」進行會審後，由召集人核定後實施，修訂時亦同。